(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 November 2001 (15.11.2001)

PCT

(10) International Publication Number
WO 01/86895 A1

(51) International Patent Classification[7]: H04L 12/58, G06F 17/60

(21) International Application Number: PCT/EP01/04747

(22) International Filing Date: 27 April 2001 (27.04.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
100 21 686.2 5 May 2000 (05.05.2000) DE

(71) Applicant *(for all designated States except US)*: **DEUTSCHE THOMSON-BRANDT GMBH** [DE/DE]; Hermann-Schwer-Str. 3, 78048 Villingen-Schwenningen (DE).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **PLATTE, Hans-Joachim** [DE/DE]; Königsberger Weg 22, 30966 Hemmingen (DE). **FLEISCHER, Wolfgang** [DE/DE]; Grosse Barlinge 37, 30171 Hannover (DE).

(74) Agent: **WÖRDEMANN, Hermes**; Deutsche Thomson-Brandt GmbH, European Patent Operations, Karl-Wiechert-Allee 74, 30625 Hannover (DE).

(81) Designated States *(national)*: AE, AG, AL, AU, BA, BB, BG, BR, CA, CN, CR, CU, CZ, DM, DZ, EE, GD, GE, HR, HU, ID, IL, IN, IS, JP, KP, KR, LC, LK, LR, LV, MA, MG, MK, MN, MX, NO, NZ, PL, RO, SG, SI, SK, TT, UA, US, UZ, VN, YU, ZA.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 01/86895 A1

(54) Title: METHOD FOR REDUCING THE SPREAD OF COMPUTER VIRUSES IN AN ELECTRONIC MAIL NETWORK

(57) Abstract: The invention relates to a method for reducing the spread of computer viruses in an electronic mail network. In a mail server having a multiplicity of connected email subscriber computers, a method is installed which is used to test emails sent in succession to the subscribers or sent in succession by the subscribers for particular commonalities, and, depending on commonalities established, either to forward the emails automatically as intended or to retain them until another criterion arises.

Method for reducing the spread of computer viruses in an electronic mail network

The invention relates to a method for reducing the spread of computer viruses in an electronic mail network.

Prior art

In today's age of electronic mails and world-wide networking of computers, many forms of so-called computer viruses constitute great danger for companies operating their networked computers with connections to the electronic outside world as well. At the points of connection to the electronic outside world, such as the Internet, special computers are operated as so-called firewalls which, amongst other things, attempt to filter out emails containing electronic viruses externally before they can reach the companies' own computers. A virus is recognized by special software which, in each case, needs to be kept at the level of the latest virus patterns by the manufacturer.

However, between the appearance of a new virus and the creation and spread of a new virus pattern, a certain time elapses in which the virus can cause considerable damage. The method of virus recognition in the firewall computer is thus fundamentally susceptible. This is because, to produce a virus pattern, it is first necessary to recognize a virus, which is usually already connected to an instance of damage. If a virus is sent by the originator and is widely introduced into company networks at the same time, then damage limitation becomes a race against the time between the spread of the virus and the creation and installation of recognition programs. Particular structures mean that the virus can cause considerable damage within a few hours, which are required to create a recognition pattern, by causing the affected computers to send copies of itself to all the

email addresses stored in this computer in snowball fashion, for example.

Invention

The aim of this invention is to limit or interrupt the snowball-like forwarding chain of the virus.

The invention is achieved by means of the features specified in Claim 1.

Advantageous developments can be found in the dependent claims.

According to the invention, in a mail server having a multiplicity of connected email subscriber computers, a method is installed which is used to test emails sent in succession to the subscribers or sent in succession by the subscribers for particular commonalities, and, depending on commonalities established, either to forward the emails automatically as intended or to retain them until another criterion arises.

The criterion which can be selected for the commonality established is the occurrence of the same subject line in a plurality of emails, the occurrence of the same text content, of an attachment which is the same, and/or the same or similarly timed sending or reception time.

If an electronic mail is automatically retained on account of one or more of these criteria, the mail server can forward an email query to the sending email subscriber to determine whether he actually wants to send all emails provided with substantial commonalities, and this sending email subscriber responds to this with an explicit acknowledgement.

Preferably, the entry of an identifier or of a password can be used as an "explicit acknowledgement" from the sending email subscriber.

An alternative or a further, "different criterion" may be an email query with the administrator of the network in question to determine whether he actually wants all emails provided with substantial commonalities to be sent, and this administrator responds to this with an explicit acknowledgement.

Preferably, such characterized electronic mails may also be forwarded after a delay time has elapsed. The time delay should then advantageously be large enough for it to be possible to react to a virus warning externally, or should fall into a prescribed time frame, for example into the normal working time of the administrator.

Patent claims

1. Method for reducing the spread of computer viruses in an electronic mail network, having a mail server and a multiplicity of email subscriber computers connected thereto, by emails sent in succession to the subscribers or sent in succession by the subscribers, characterized in that the emails sent in succession to the subscribers or sent in succession by the subscribers are tested for particular commonalities and, depending on commonalities established, the electronic emails are either automatically forwarded as intended or are retained until another criterion arises.

2. Method according to Claim 1, characterized in that the criterion used for the commonality established is the occurrence of the same subject line in a plurality of emails, the occurrence of the same text content, of an attachment which is the same, and/or the same or similarly timed sending or reception time.

3. Method according to Claim 1, characterized in that, if an electronic mail is automatically retained on account of one or more of these criteria, the mail server forwards an email query to the sending email subscriber.

4. Method according to Claim 3, characterized in that these emails provided with substantial commonalities are sent by the mail server if the sending email subscriber acknowledges the email query by the email server with an explicit acknowledgement.

5. Method according to Claim 4, characterized in that the entry of an identifier or of a password is

preferably used as an "explicit acknowledgement" from the sending email subscriber.

6. Method according to Claim 1, characterized in that, as a further, different criterion, an email query is sent to the administrator of the network in question to determine whether he actually wants all emails provided with substantial commonalities to be sent, and this administrator responds to this with an explicit acknowledgement.

7. Method according to Claim 1, characterized in that such characterized electronic mails are forwarded after a delay time has elapsed.

8. Method according to Claim 7, characterized in that the time delay falls into a prescribed time frame, preferably into the normal working time of the administrator.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 01/04747

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L12/58 G06F17/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC, COMPENDEX

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6 052 709 A (PAUL SUNIL) 18 April 2000 (2000-04-18) abstract column 1, line 52 -column 3, line 13	1-8
A	WO 97 39399 A (TREND MICRO INC; CHEN EVA (US)) 23 October 1997 (1997-10-23) page 4, line 29 -page 5, line 25	1-8
A	WO 99 67731 A (MICROSOFT CORP) 29 December 1999 (1999-12-29) page 10, line 28 -page 11, line 29	1-8

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
4 October 2001	12/10/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax (+31–70) 340–3016	Sigolo, A

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP 01/04747

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
US 6052709	A	18-04-2000	AU	1631199 A	12-07-1999
			EP	1040584 A2	04-10-2000
			WO	9933188 A2	01-07-1999
WO 9739399	A	23-10-1997	US	5889943 A	30-03-1999
			AU	2556697 A	07-11-1997
			EP	0954794 A2	10-11-1999
			JP	2000517440 T	26-12-2000
			WO	9739399 A2	23-10-1997
WO 9967731	A	29-12-1999	US	6161130 A	12-12-2000
			EP	1090368 A1	11-04-2001
			WO	9967731 A1	29-12-1999